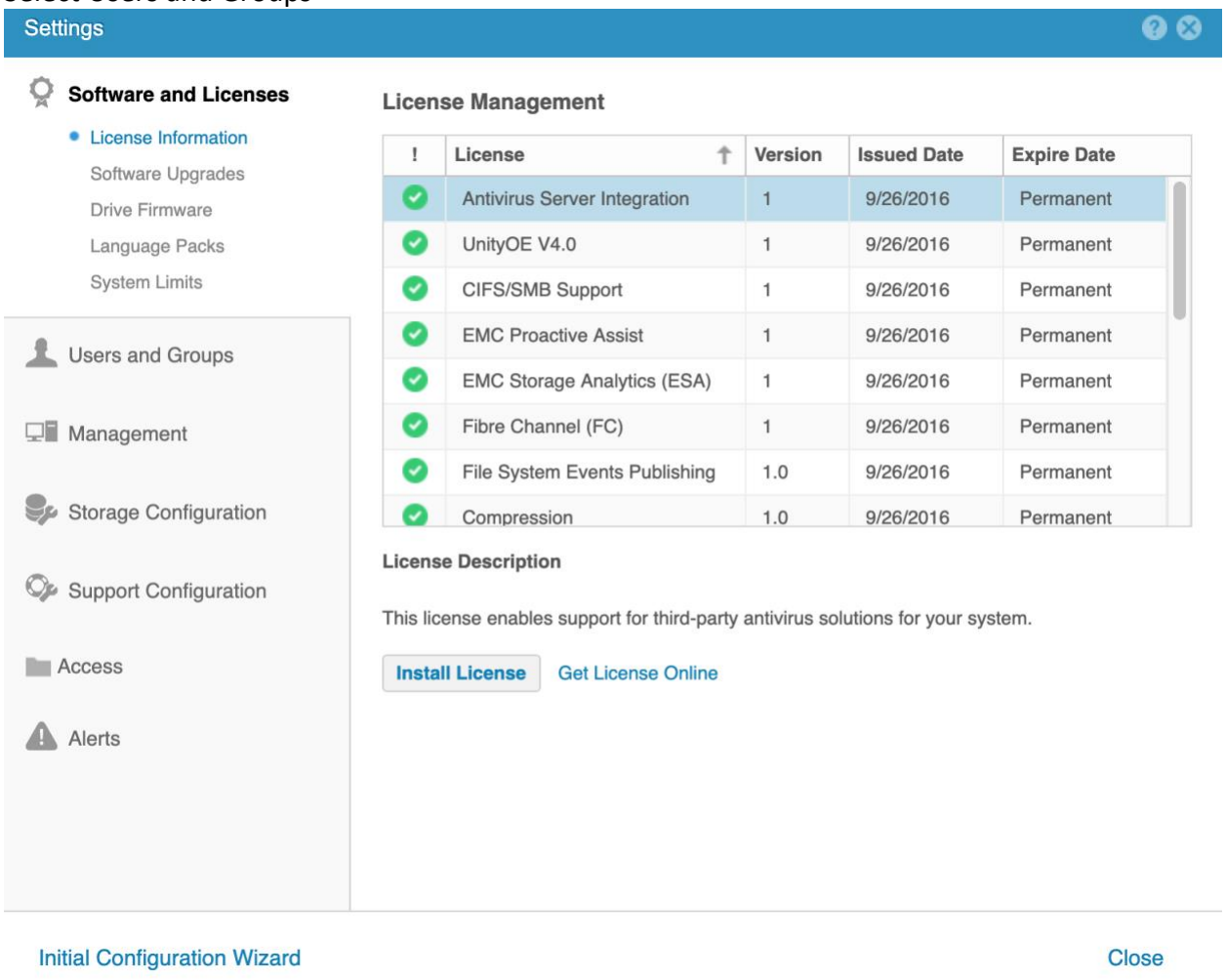
Dell EMC Unity Configuration Guide 4.0.1(d)

1) Configure Directory Services for Unity

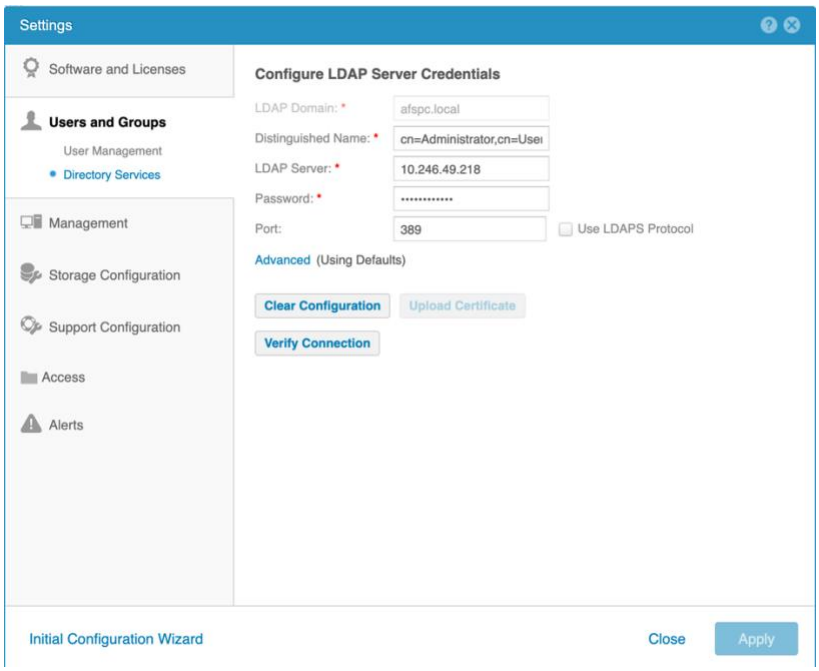
Log into Unity with Local User

Click the “Update System Settings Widget” on the top right by the user Icon.
Select Users and Groups

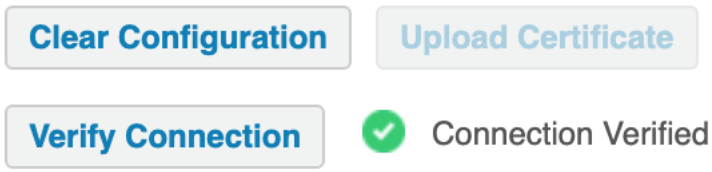


Select “Directory Services”

- Configure Distinguished Name for instance:- cn=Administrator,cn=Users,dc=afspc,dc=local
- LDAP Server: <THEIPADDRESSOFYOURDIRECTORYSERVER>
- Password: The Password of the User that will connect to the Directory Server
- Port 389 (or 636 if Secure)..
- Select “Verify Connection… and ensure a successful test

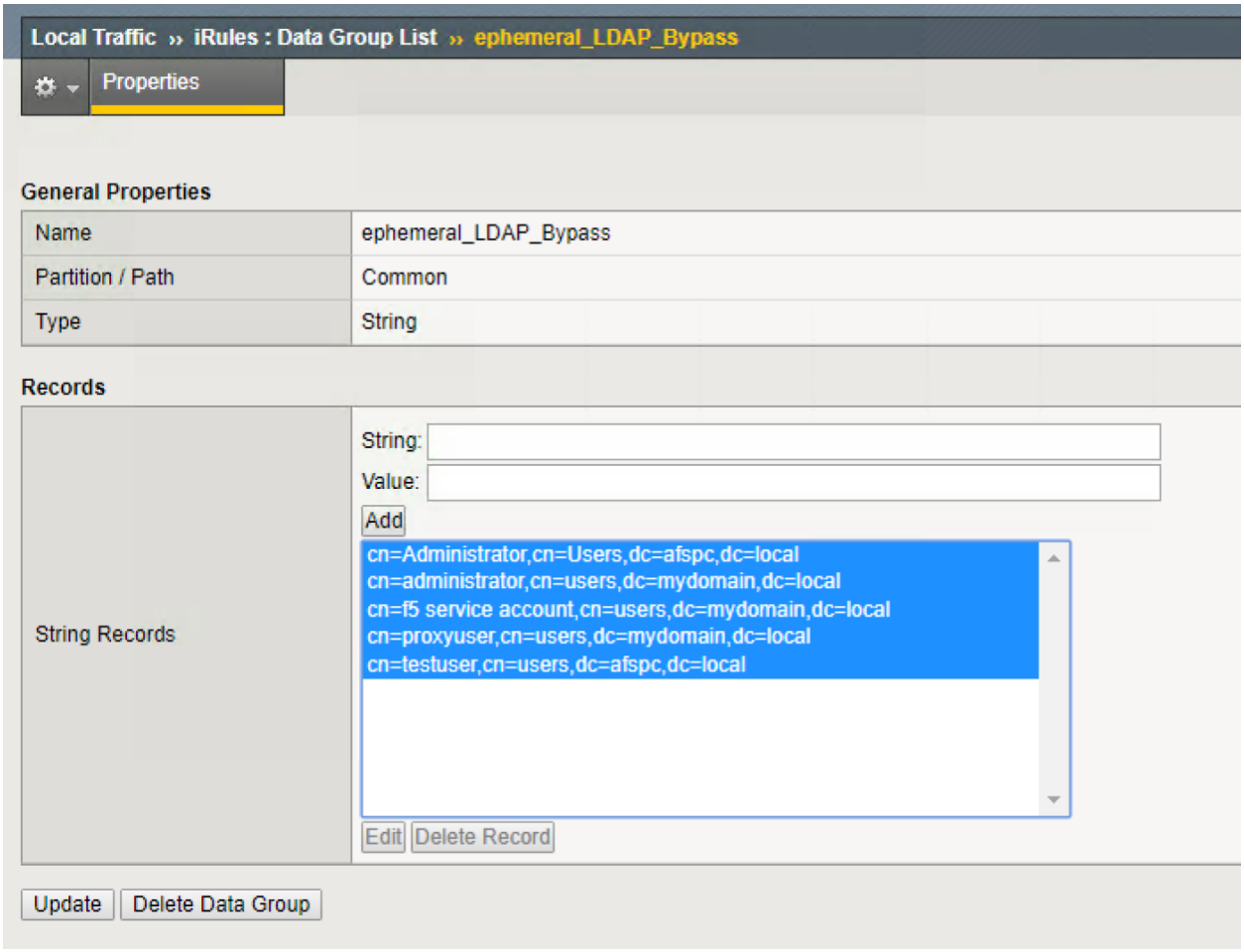


.



Logout of the Unity Server.. and then Log Back in with an Active Directory User to verify that you can login to the system with an AD User directly the Unity User Interface (no Big-IP)

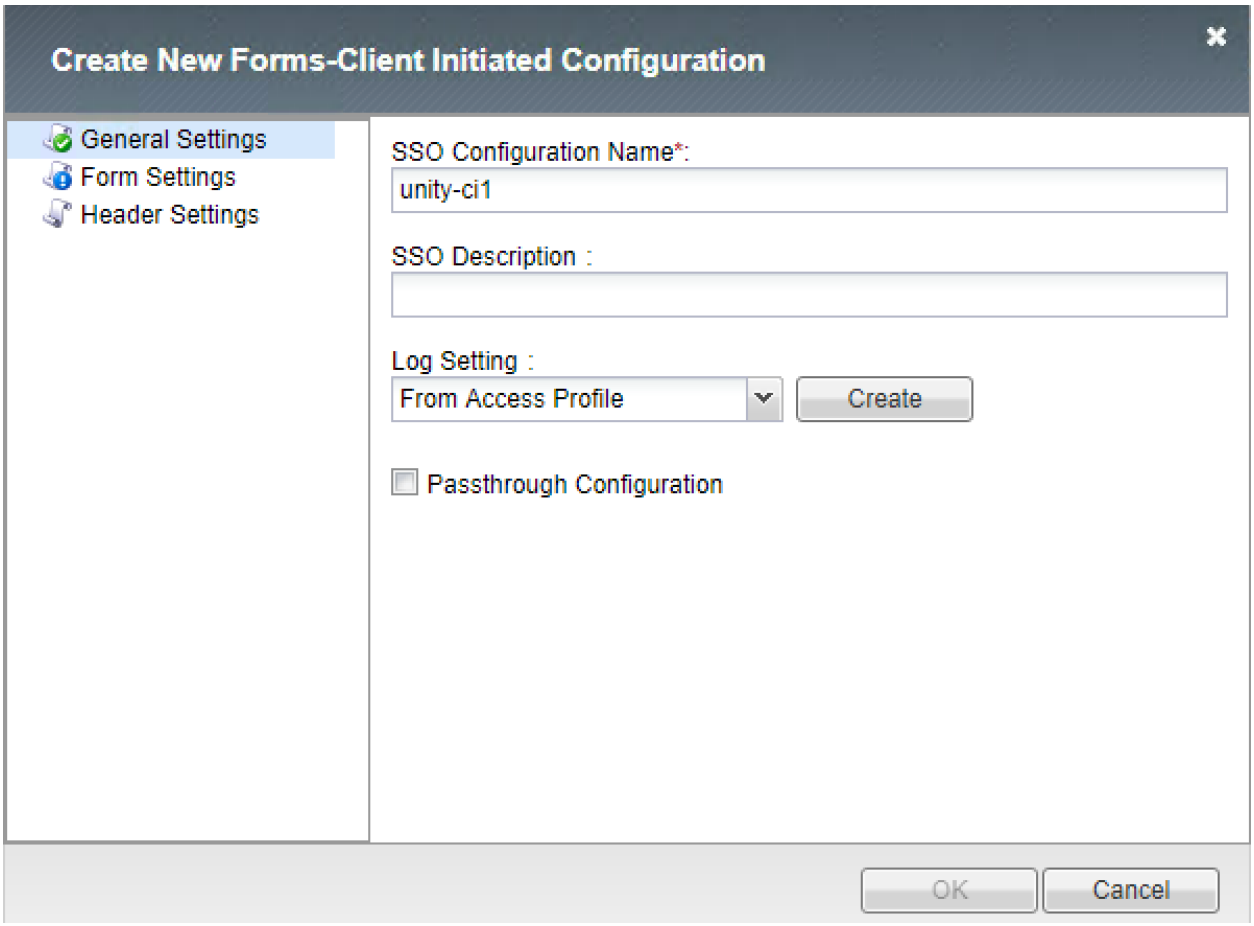
Note: The DN that username translates to must be in the ephemeral_LDAP_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List



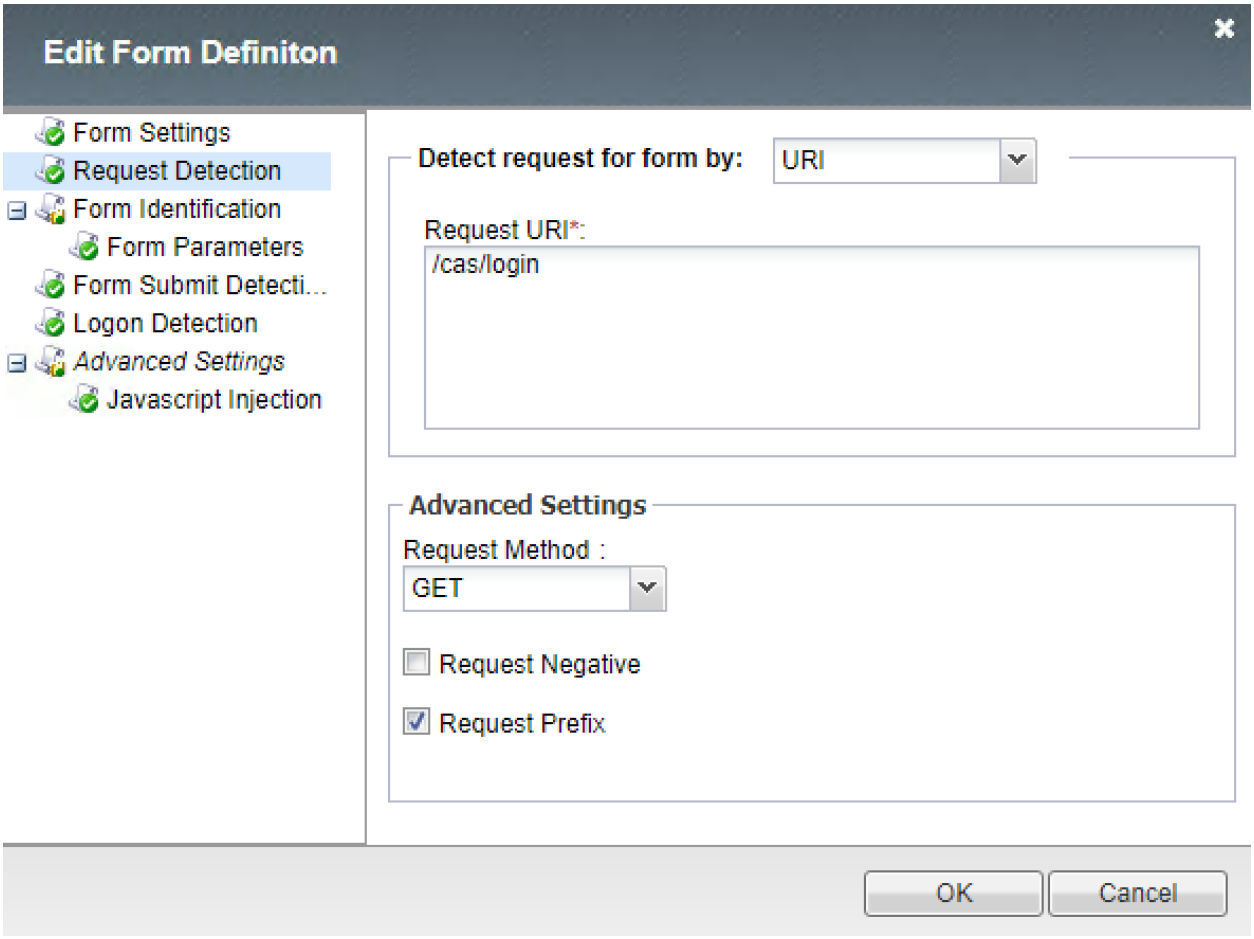
2) Create an SSO Configuration for Unity

A. Create a single sign on policy for Unity.

- Go to Access/Single Sign-On/Forms – Client Initiated
- Provide A name Under “SSO Configuration Name”

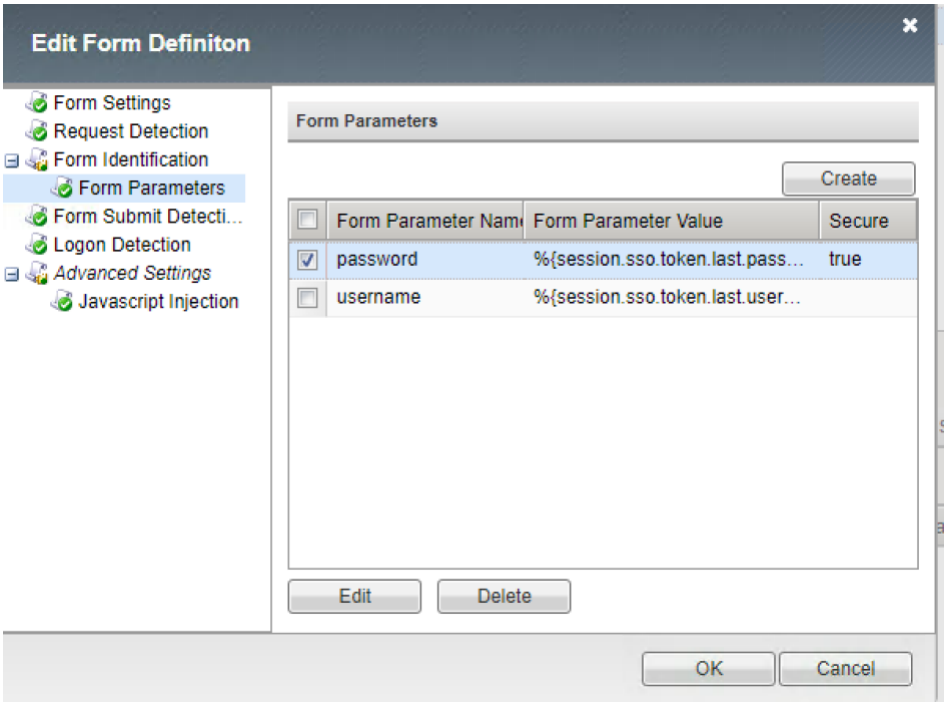


- Click Form Settings
  - Click Create
- Provide a Form Name "frm1"
  - Click "Request Detection
    - Detect Request form by URI
    - Request URI: /cas/login
    - Request Method GET
    - Request Prefix needs to be "checked"

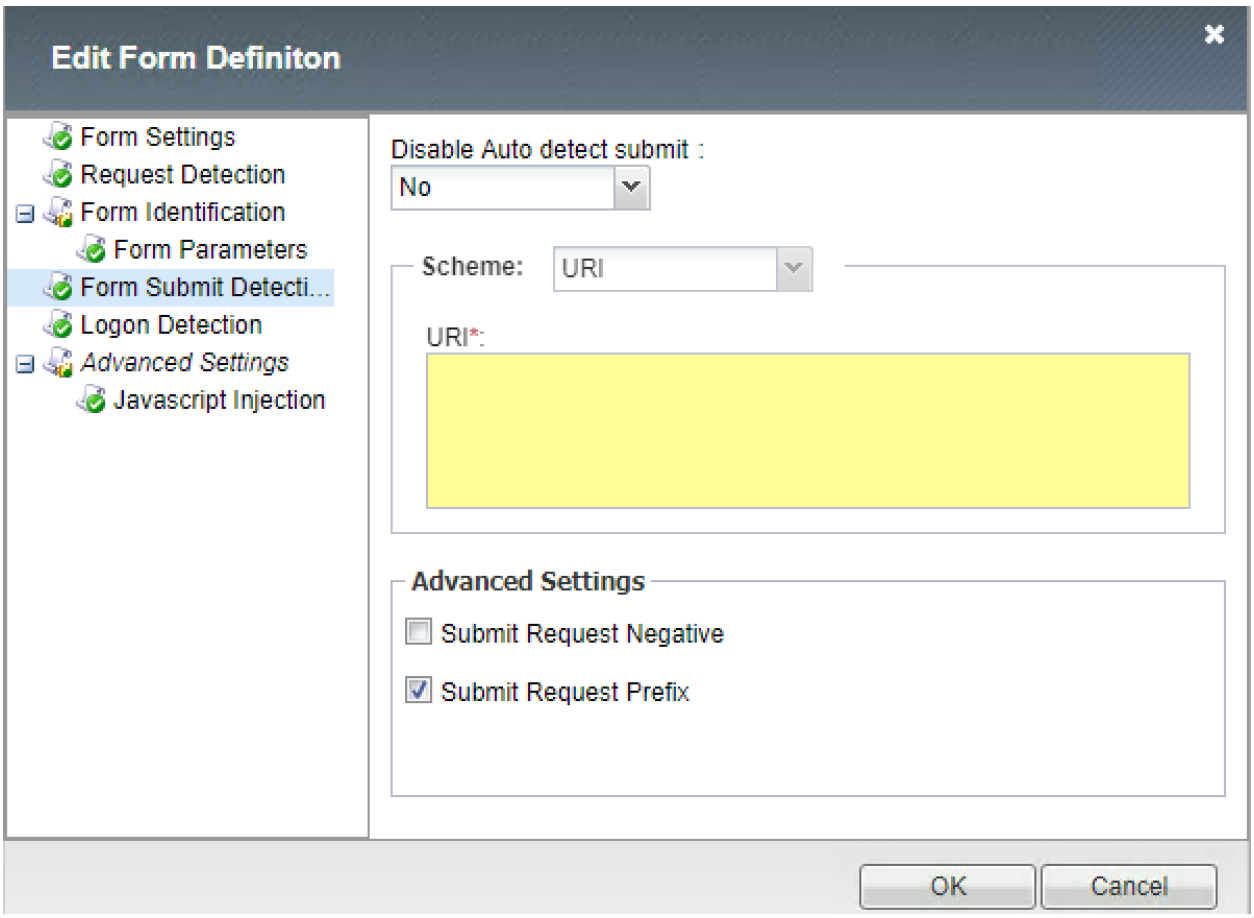


- Click on Form Parameters
  - Associated Form Parameters with APM Form Parameter Values.
    - Parameter Name:- password
    - Form Parameter Value: - %{session.sso.token.last.password}
    - Secure: Yes

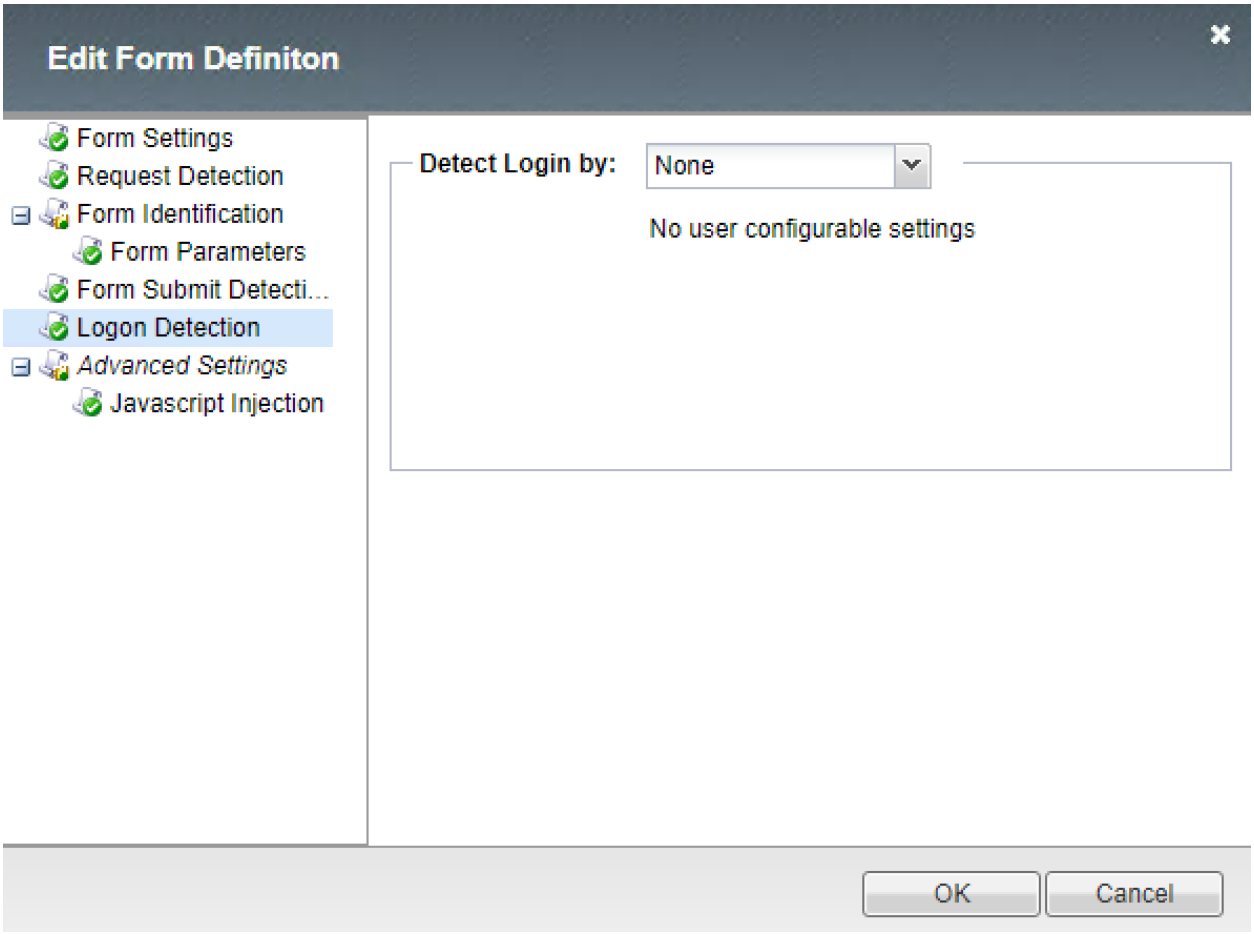
    - Form Parameter Name:- username
    - Form Parameter Value:- %{session.sso.token.last.username}
    - Secure: No



- Form Submit Detection
  - Disable Auto detect submit:NO
  - Submit Request Prefix “Checked”



- Logon Detection



- Click Javascript Injection
  - Click Custom
  - Enter Custom JavaScript

```
<script>

 function __f5submit() {

   document.getElementById("password").value =
'%{session.custom.ephemeral.last.password_sso}';

   document.getElementById("username").value = '%{session.custom.ephemeral.upn}';

   document.getElementById("submit").click();

 }
```

```
if (window.addEventListener) {

 window.addEventListener('load',__f5submit,false);

} else if (window.attachEvent) {

 window.attachEvent('onload',__f5submit);

} else {

 window.onload=__f5submit;

}




</script>
```

3) Create Portal Access Resource for Unity

- In the APM menu select Connectivity / VPN : Portal Access : Portal Access Lists
  - Click Create
  - Name: Your choice “Unity” for example
  - Leave Patching to be default.
  - Application URI: Needs to be the IP or hostname of the Unity Server

General Properties

Name	Unity
Partition / Path	Common
Description	
ACL Order	1

Configuration: Basic

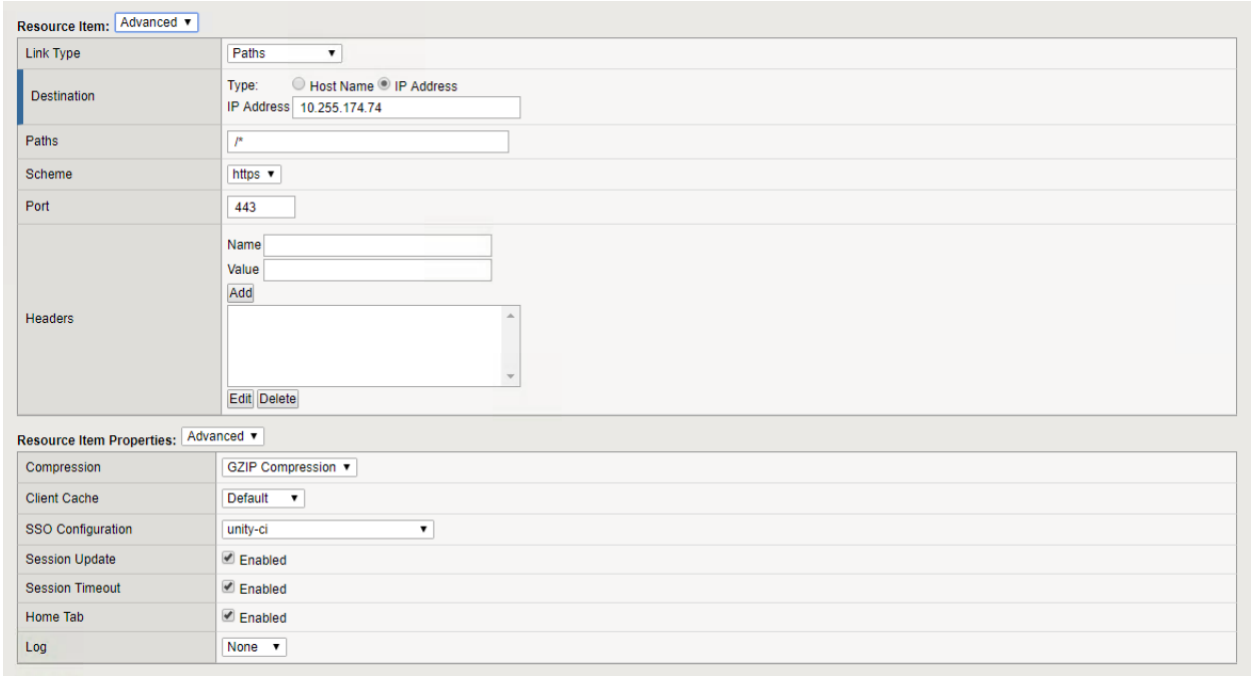
Match Case For Paths	Yes
Patching	Type Full Patching HTML Patching JavaScript Patching CSS Patching Flash Patching Java Patching
Publish on Webtop	Enable
Link Type	Application URI
Application URI	https://10.255.174.74/

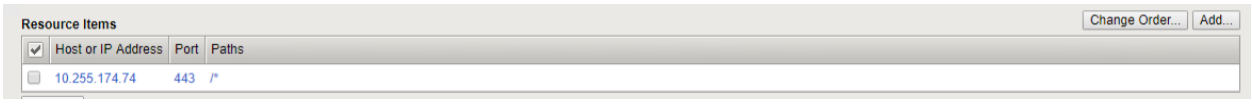
Customization Settings for English

Language	English
Caption	Unity GUI
Detailed Description	
Image	Choose File No file chosen View/Hide Restore Default

Update Delete

- Create a Resource Item within the portal Access Resource.
    - For resource type use the IP Address or Host Name depending upon how you are configured in your environment.
    - The IP Address/Hostname will be the IP Address or Hostname of the back end resource. Meaning the IP Address or host name of the unity server.
    - For Link Type Select “Paths”
    - For the Paths Entry Field type /*
    - Scheme = https
    - Compression: GZIP Compression
    - Client Cache: Default
    - SSO Configuration: unity-ci (The SSO Configuration would have been created in the previous step.





4) You can then associate the portal access resource item with the Webtop Policy.

- Click Access/Profiles
- Click “Edit” under Per-Session Policy
- Select the Webtop. This will be associated with an “Advanced Resource Assign Webtop Item”
- Then Select the Add/Delete Button
- Then select the Portal Access Tab
- Then Select the Portal Access webtop Item that you want to display on the webtop… for Example. “Unity”